EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	15	provid$4 and restrict$4 and transm$6 and configerat$4 adj file and maintain$3 and TFTP and us$3 and DHCP adj server and associate and un adj modified and CM configeration and filename and IP adj address and receipt and DHCP adj REQUEST and stor$3 and coordination adj pass adj phrase and generat$4 first adj authentication adj key and creat$3 and modif$5 combin$3 and authentication adj key and transmit$4 and DHCP adj RESPONSE and TFTP and server and pars$3 and second adj authentication adj key and match$3 and depend not adj known.clm.	US-PGPUB	OR	ON	2007/08/16 16:18
L2	411626	provid$4 with restrict$4 with transm$6 with configerat$4 adj file with maintain$3 with TFTP with us$3 with DHCP adj server with associate with un adj modified with CM configeration with filename with IP adj address with receipt with DHCP adj REQUEST with stor$3 with coordination adj pass adj phrase with generat$4 first adj authentication adj key with creat$3 with modif$5 combin$3 with authentication adj key with transmit$4 v DHCP adj RESPONSE with TFTP with server with pars$3 with second adj authentication adj key with match$3 with depend not adj known.clm.	US-PGPUB	OR	ON	2007/08/16 16:21
L3	134998	l2 and @py<"2004"	US-PGPUB	OR	ON	2007/08/16 16:30
L4	7414	713/200	US-PGPUB; USPAT	OR	ON	2007/08/16 16:30
L5	1	l1 and L4	US-PGPUB	OR	ON	2007/08/16 16:31
L6	305	726/4	US-PGPUB; USPAT	OR	ON	2007/08/16 16:31
L7	0	l1 and L6	US-PGPUB	OR	ON	2007/08/16 16:31
L8	80	726/18	US-PGPUB; USPAT	OR	ON	2007/08/16 16:31
L9	0	l1 and L8	US-PGPUB	OR	ON	2007/08/16 16:31

EAST Search History

L10	138	726/21	US-PGPUB; USPAT	OR	ON	2007/08/16 16:31
L11	0	l1 and L10	US-PGPUB	OR	ON	2007/08/16 16:32
L12	2961	713/168	US-PGPUB; USPAT	OR	ON	2007/08/16 16:32
L13	4	l1 and L12	US-PGPUB	OR	ON	2007/08/16 16:34
L14	159	380/229	US-PGPUB; USPAT	OR	ON	2007/08/16 16:34
L15	0	l1 and L14	US-PGPUB	OR	ON	2007/08/16 16:35
L16	783	705/67	US-PGPUB; USPAT	OR	ON	2007/08/16 16:35
L17	0	l1 and L16	US-PGPUB	OR	ON	2007/08/16 16:35
L18	174	l2 and L4	US-PGPUB	OR	ON	2007/08/16 16:36
L19	0	l2 and L6	US-PGPUB	OR	ON	2007/08/16 16:36
L20	0	l2 and L8	US-PGPUB	OR	ON	2007/08/16 16:36
L21	0	l2 and L10	US-PGPUB	OR	ON	2007/08/16 16:36
L22	123	l2 and L12	US-PGPUB	OR	ON	2007/08/16 16:37
L23	1	l2 and L14	US-PGPUB	OR	ON	2007/08/16 16:37
L24	11	l2 and L16	US-PGPUB	OR	ON	2007/08/16 16:37
S1	16	"6598057"	US-PGPUB; USPAT	OR	ON	2007/08/16 15:54
S2	1	10/613659	US-PGPUB; USPAT	OR	ON	2007/08/14 16:13
S3	81	first adj authentication adj key	US-PGPUB; USPAT	OR	ON	2007/08/14 16:13
S4	71	second adj authentication adj key	US-PGPUB; USPAT	OR	ON	2007/08/14 16:32
S5	61	S3 and S4	US-PGPUB; USPAT	OR	ON	2007/08/14 16:14
S6	7414	713/200	US-PGPUB; USPAT	OR	ON	2007/08/14 16:15
S7	5	S5 and S6	US-PGPUB; USPAT	OR	ON	2007/08/14 16:31
S8	6726	dhcp	US-PGPUB; USPAT	OR	ON	2007/08/14 16:31
S9	1395	tftp	US-PGPUB; USPAT	OR	ON	2007/08/14 16:31
S10	717	S8 and S9	US-PGPUB; USPAT	OR	ON	2007/08/14 16:31
S11	1	S10 and S5	US-PGPUB; USPAT	OR	ON	2007/08/15 08:23

S12	3887	authentication adj key	US-PGPUB; USPAT	OR	ON	2007/08/14 16:32
S13	9	S10 and S12	US-PGPUB; USPAT	OR	ON	2007/08/14 16:57
S14	747	dhcp adj request	US-PGPUB; USPAT	OR	ON	2007/08/14 16:58
S15	216	dhcp adj response	US-PGPUB; USPAT	OR	ON	2007/08/14 16:58
S16	6	S14 adj S15	US-PGPUB; USPAT	OR	ON	2007/08/15 08:28
S17	320	tftp adj server	US-PGPUB; USPAT	OR	ON	2007/08/14 17:09
S18	0	S16 and S17	US-PGPUB; USPAT	OR	ON	2007/08/14 17:09
S19	3323	dhcp adj server	US-PGPUB; USPAT	OR	ON	2007/08/14 17:10
S20	192	S17 and S19	US-PGPUB; USPAT	OR	ON	2007/08/14 17:10
S21	0	S20 and S16	US-PGPUB; USPAT	OR	ON	2007/08/14 17:11
S22	1	S20 and S5	US-PGPUB; USPAT	OR	ON	2007/08/14 17:11
S23	2	S20 and S12	US-PGPUB; USPAT	OR	ON	2007/08/14 17:16
S24	587283	match	US-PGPUB; USPAT	OR	ON	2007/08/14 17:16
S25	75	S24 and S20	US-PGPUB; USPAT	OR	ON	2007/08/14 17:16
S26	22	S25 and @py<"2004"	US-PGPUB; USPAT	OR	ON	2007/08/15 07:10
S27	1	09/470105	US-PGPUB; USPAT	OR	ON	2007/08/15 07:10
S28	1395	tftp	US-PGPUB; USPAT	OR	ON	2007/08/15 08:23
S29	747	dhcp adj request	US-PGPUB; USPAT	OR	ON	2007/08/15 08:23
S30	216	dhcp adj response	US-PGPUB; USPAT	OR	ON	2007/08/15 08:23
S31	6	S29 adj S30	US-PGPUB; USPAT	OR	ON	2007/08/15 08:23
S32	0	S28 and S31	US-PGPUB; USPAT	OR	ON	2007/08/15 08:23
S33	8	09/800803	US-PGPUB; USPAT	OR	ON	2007/08/15 08:35

EAST Search History

S34	4	09/018400	US-PGPUB; USPAT	OR	ON	2007/08/15 13:17
S35	61	"5870134"	US-PGPUB; USPAT	OR	ON	2007/08/15 17:17
S36	27	"5506905"	US-PGPUB; USPAT	OR	ON	2007/08/15 17:32
S37	8	09/800803	US-PGPUB; USPAT	OR	ON	2007/08/15 18:17
S38	304	726/4	US-PGPUB; USPAT	OR	ON	2007/08/15 18:17
S39	80	726/18	US-PGPUB; USPAT	OR	ON	2007/08/15 18:17
S40	138	726/21	US-PGPUB; USPAT	OR	ON	2007/08/15 18:17
S41	2954	713/168	US-PGPUB; USPAT	OR	ON	2007/08/15 18:18
S42	27	713/155-159	US-PGPUB; USPAT	OR	ON	2007/08/15 18:18
S43	158	380/229	US-PGPUB; USPAT	OR	ON	2007/08/15 18:18
S44	783	705/67	US-PGPUB; USPAT	OR	ON	2007/08/15 18:28
S45	0	coordination adj passphrase	US-PGPUB; USPAT	OR	ON	2007/08/15 18:29
S46	1	coordination adj pass adj phrase	US-PGPUB; USPAT	OR	ON	2007/08/15 18:29

10/69,K/6 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

0010262820 - Drawing available
WPI ACC NO: 2000-575421/200054
XRPX Acc No: N2000-425871

Asynchronous input-output cache memory has pair of circuits for accessing system data bus and input-output data bus respectively, based on data stored in data memory area

Patent Assignee: HEWLETT-PACKARD CO (HEWP); HEWLETT-PACKARD DEV CO LP (HEWP)
Inventor: MONISH; THOMAS; SHAH M S; SPENCER T V

Patent Family (2 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	
JP 2000227877	A	20000815	JP 1999360373	A	19991220	200054	B
US 7035981	B1	20060425	US 1998218333	A	19981222	200628	E

Priority Applications (no., kind, date): US 1998218333 A 19981222

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
JP 2000227877	A	JA	10	4	

Alerting Abstract JP A

NOVELTY - The cache has data memory area (120) for communicating with system data bus and input-output data bus, simultaneously. Based on the data stored in memory area, a pair of circuits access input-output data bus and system bus, respectively.

USE - In e.g. asynchronous input-output cache memory.

ADVANTAGE - Queuing time in both system optical frequency domain and input-output frequency domain is reduced due to the presence of the pair of circuits.

DESCRIPTION OF DRAWINGS - The figure shows the block diagram of asynchronous input-output cache memory.

120 Data memory area

Title Terms/Index Terms/Additional Words: ASYNCHRONOUS; INPUT; OUTPUT; CACHE; MEMORY; PAIR; CIRCUIT; ACCESS; SYSTEM; DATA; BUS; RESPECTIVE; BASED; STORAGE; AREA

Class Codes

International Classification (Main): G06F-012/08
International Classification (+ Attributes)
IPC + Level Value Position Status Version
G06F-0013/00 A I F B 20060101
US Classification, Issued: 711144000, 711145000, 711141000, 711147000, 711167000, 711130000, 711162000, 709400000, 713400000, 713502000, 713600000, 710019000, 710027000, 710055000, 710061000, 710107000, 710125000, 710200000, 710240000, 710244000, 710305000

File Segment: EPI;
DWPI Class: T01
Manual Codes (EPI/S-X): T01-H05B2

Original Publication Data by Authority

Original Abstracts:

The present invention is generally directed to a device including an asynchronous **input** /output (I/O) **data** cache. The **device** **includes** a single **data** storage area that **is** disposed in communication with both a system data bus and a I/O **data** bus. Similarly, the **device** includes an **address** **storage** area that **is** configured to store system **addresses** corresponding to **data** contemporaneously stored in the **data** storage area. The **device** further includes a **first** circuit configured to **indicate** **validity** **status** of **data** within the data storage area for immediate access from the I/O data bus. A similar, second circuit is also included and configured to indicate validity **status** of **data** within the data storage area for immediate access from the system data bus. In accordance...

...I/O data bus, and providing a single address storage area configured to store system **memory** addresses corresponding to **data** contemporaneously stored in the data storage area. In accordance with the broad aspect of the ...

Claims:

...communication with both a system data bus and an I/O data bus, wherein the **data** storage area is **configured** **to** store a non- **duplicative** **data** set;a **single** address storage area **configured** to **store** system addresses corresponding to **data** contemporaneously stored in **the** **data** storage area;a first circuit **configured** to indicate validity status of data within the **data** storage **area** for **immediate** **access** from **the** I/O data bus; and **a** **second** circuit **configured** to **indicate** **validity** status of data within the data storage area for **immediate** access **from** the system **data** bus, wherein **the** **second** circuit **is** **configured** such that the validity status of the data stored within the **data** storage area **never** appears valid from the I/O data bus, without first appearing valid from the system...

```
10/69,K/7     (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2007 The Thomson Corporation. All rts. reserv.

0009182557  - Drawing available
WPI ACC NO: 1999-106394/199909
XRPX Acc No: N1999-076789
Telecommunication system secure service connection - By encrypting data
transmitted via secure connection using encrypting algorithm
Patent Assignee: SONERA OY  (SONE-N); SONERA OYJ  (SONE-N); TELECOM FINLAND
  OY  (TELE-N); TELIASONERA FINLAND OYJ  (TELI-N); SONERA SMARTTRUST OY
  (SONE-N)
Inventor: VATANEN H
Patent Family (12 patents,  81 countries)
Patent                          Application
Number          Kind   Date     Number          Kind   Date     Update
WO 1999001990    A2   19990114  WO 1998FI532      A   19980618  199909  B
FI 199702819     A    19981231  FI 19972819       A   19970630  199920  E
AU 199877717     A    19990125  AU 199877717      A   19980618  199923  E
EP 1027806       A2   20000816  EP 1998925695     A   19980618  200040  E
                                WO 1998FI532      A   19980618
US 6237093       B1   20010522  WO 1998FI532      A   19980618  200130  E
                                US 1999474409     A   19991229
AU 739814        B    20011018  AU 199877717      A   19980618  200174  E
NZ 502187        A    20011130  NZ 502187         A   19980618  200207  E
                                WO 1998FI532      A   19980618
JP 2002511994    W    20020416  WO 1998FI532      A   19980618  200242  E
                                JP 1999506485     A   19980618
EP 1027806       B1   20051123  EP 1998925695     A   19980618  200577  E
                                WO 1998FI532      A   19980618
DE 69832517      E    20051229  DE 69832517       A   19980618  200603  E
                                EP 1998925695     A   19980618
                                WO 1998FI532      A   19980618
DE 69832517      T2   20060727  DE 69832517       A   19980618  200649  E
                                EP 1998925695     A   19980618
                                WO 1998FI532      A   19980618
FI 117366        B1   20060915  FI 19972819       A   19970630  200662  E

Priority Applications (no., kind, date): FI 19972819  A  19970630

Patent Details
Number          Kind  Lan   Pg   Dwg  Filing Notes
WO 1999001990    A2   EN    11    1
National Designated States,Original:  AL AM AT AU AZ BA BB BG BR BY CA CH
   CN CU CZ DE DK EE ES FI GB GE GH GM GW HU ID IL IS JP KE KG KP KR KZ LC
   LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL
   TJ TM TR TT UA UG US UZ VN YU ZW
Regional Designated States,Original:  AT BE CH CY DE DK EA ES FI FR GB GH
   GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW
AU 199877717     A    EN              Based on OPI patent   WO 1999001990
EP 1027806       A2   EN              PCT Application  WO 1998FI532
                                      Based on OPI patent   WO 1999001990
Regional Designated States,Original:  AT BE CH CY DE DK ES FI FR GB GR IE
   IT LI LT LU LV MC NL PT SE
US 6237093       B1   EN              Continuation of application  WO
   1998FI532
AU 739814        B    EN              Previously issued patent  AU 9877717

                                      Based on OPI patent   WO 1999001990
NZ 502187        A    EN              PCT Application  WO 1998FI532
                                      Based on OPI patent   WO 1999001990
```

```
JP 2002511994    W   JA    14       PCT Application  WO 1998FI532
                                    Based on OPI patent   WO 1999001990
EP 1027806       B1  EN             PCT Application  WO 1998FI532
                                    Based on OPI patent   WO 1999001990
Regional Designated States,Original:  AT BE CH CY DE DK ES FI FR GB GR IE
   IT LI LT LU LV MC NL PT SE
DE 69832517      E   DE             Application  EP 1998925695
                                    PCT Application  WO 1998FI532
                                    Based on OPI patent   EP 1027806
                                    Based on OPI patent   WO 1999001990
DE 69832517      T2  DE             Application  EP 1998925695
                                    PCT Application  WO 1998FI532
                                    Based on OPI patent   EP 1027806
                                    Based on OPI patent   WO 1999001990
FI 117366        B1  FI             Previously issued patent  FI 9702819
```

Alerting Abstract WO A2

Method is for a system with telecommunication networks (1,3), terminal devices (2,4) and telecommunication server (5). Device (1) is connected via telecommunication connection (6) to the telecommunication server (5) and device (3) is connected to the server (5) via second telecommunication connection (7). The unique **address** of **device** (2) and the **data** needed for **verification** of information giving **device** (**2**) **access** to server (5) services are transmitted via **device** (4). The **data** sent by **device** (4) is verified and connection (6) is set up based on the **verification** and **address** **data** received if **device** (**2**) has the required right of access to the server services.

USE - Method is for setting up a secure service connection in a telecommunication system e.g. the Internet and a telephone network or mobile communication network.

ADVANTAGE - Method allows reliable user identification and allows him to order services offered by the network.

Title Terms/Index Terms/Additional Words: TELECOMMUNICATION; SYSTEM; SECURE ; SERVICE; CONNECT; DATA; TRANSMIT; ALGORITHM

Class Codes

International Classification (Main): H04M-011/00, H04Q-001/00
(Additional/Secondary): H04L-012/66, H04Q-007/22, H04Q-007/24, H04Q-007/26 , H04Q-007/30, H04Q-007/38

```
International Classification (+ Attributes)
IPC + Level Value Position Status Version
  H04L-0029/06  A  I     R  20060101
  H04Q-0001/00  A  I  F  B  20060101
  H04L-0012/22  A  I  F     20060101
  H04M-0011/00  A  I  L     20060101
  H04L-0029/06  C  I     R  20060101
```

US Classification, Issued: 713168000, 713182000, 380255000, 713162000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-H07C5S; T01-J08C; W01-A05B; W01-C02B6A; W01-C05B3B

Alerting Abstract ...device (3) is connected to the server (5) via second telecommunication connection (7). The unique **address** of **device** (2) and the **data** needed for **verification** of information giving **device** (**2**) **access** to server (5) services are transmitted via **device** (4). The **data** sent by **device** (4) is verified and connection (6) is set up based on the

verification and **address** **data** received if **device** (**2**) has the required right of access to the server services...

Original Publication Data by Authority

Original Abstracts:
...telecommunication connection (7). In an embodiment of the invention,the unique address of the first **terminal** **device** (**2**) **and** the **data** needed for the **verification** of information giving **the** **first** terminal **device** (2) **access** to the **services** of the telecommunication server (5) are transmitted via the second terminal device (4); the data sent by the **second** terminal **device** are **verified** in **the** telecommunication **server** ; and the **first** telecommunication connection (6) from the telecommunication server to the first terminal device is **set** up **based** on the **verification** **and** the address **data** received if **the** **first** terminal **device** has **the** required right of access to the services of the telecommunication server...

...terminal device is connected to the telecommunication server via a second telecommunication connection. The unique **identifying** address of the **first** terminal **device** and the **data** needed **to** **verify** that the **first** terminal **device** is permitted **access** to **the** services of the telecommunication server are transmitted to the telecommunication server via the second terminal device and second telecommunication connection, **and** the **data** sent by the **second** **terminal** **device** are **verified** at the **telecommunication** server. **If** the **first** terminal **device** is determined **to** have the required right of access to the services of the telecommunication server, the first telecommunication connection from the telecommunication server to the first terminal device is set **up** **based** **on** the successful **verification** **and** using the address data received by the telecommunication server...

...connection (7). In an embodiment of the invention,the unique address of the first terminal **device** (2) and the **data** needed for **the** **verification** **of** **information** giving the **first** terminal **device** (**2**) **access** to the services of the telecommunication server (5) are transmitted via the second terminal **device** (4); the **data** sent by the **second** terminal **device** are **verified** **in** the telecommunication server; **and** the **first** telecommunication **connection** (6) from the telecommunication server to the first terminal device is set up **based** on the **verification** and **the** address **data** received if the **first** **terminal** **device** has **the** **required** right of access to the services of the telecommunication server...
Claims:
...encrypted message packets;</br> transmitting via the second terminal device (4) the unique address of the **first** **terminal** **device** (**2**) and **information** **authorizing** the use of services and/or ordering of services to the telecommunication **server** (5);</br> **verifying** the **data** sent **by** the **second** **terminal** **device** (**4**) in the **telecommunication** **server** (5); and</br> **setting** **up** the first telecommunication connection (6) from the telecommunication server to the **first** **terminal** **device** (2) **based** on the **verification** and **the** **address** **data** received if the first terminal device (2) has the required right of access to use and/or order the services **of** the **telecommunication** **server** (**5**).

...<b>5</b>), via the second terminal device (<b>4</b>) and the second telecommunication connection (<b>7</b>), a unique **identifying** address of the **first** terminal **device**0 (**<b>2</b>**) and data permitting **verification** by the telecommunication **server** as **to** whether **the first** terminal device (<b>2</b>) is permitted access to a service provided by the telecommunication server (<b>5</b>);verifying, at the telecommunication server (<b>5</b>), the **data** sent to the telecommunication server via the second terminal device (<b>4</b>) and the second telecommunication...

...device (<b>2</b>) is permitted access to the service provided by the telecommunication server; andestablishing, **where** said **verifying** step **determines** that **the first** terminal **device** (<b>2</b>) is permitted **access** to the service, the first telecommunication connection (<b>6</b>) between the first terminal device (<b>3</b>) and the telecommunication server (<b>5</b>) using the unique **identifying** address of the **first** terminal **device** (**<b>2</b>**) **received** by the telecommunication server (<b>5</b>) from the second **terminal device.**>

10/69,K/4 (Item 4 from file: 350)
DIALOG(R)File 350:Derwent WPIX

0014763117 - Drawing available
WPI ACC NO: 2005-110771/200512
XRPX Acc No: N2005-095681

Cable modem **transmission restriction method for use with e.g. personal computer, involves transmitting** configuration file **to** cable modem **only if authentication keys generated based on** configuration file **match with each other**

Patent Assignee: DANFORTH A (DANF-I); GOULD K (GOUL-I); TIME WARNER CABLE INC (TIME-N)

Inventor: DANFORTH A; GOULD K

Patent Family (2 patents, 2 countries)

Patent			Application				
Number	Kind	Date	Number	Kind	Date	Update	
US 20050005154	A1	20050106	US 2003613659	A	20030703	200512	B
CA 2473326	A1	20060108	CA 2473326	A	20040708	200612	NCE

Priority Applications (no., kind, date): CA 2473326 A 20040708; US 2003613659 A 20030703

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20050005154	A1	EN	22	9	
CA 2473326	A1	EN			

Alerting Abstract US A1

NOVELTY - An unmodified **cable modem** (CM) **configuration filename** is associated to a CM internet protocol (IP) address and an authentication key is generated. A modified CM **configuration filename** is generated by combining previous filename with the key. The modified filename is parsed to unmodified filename by which a new authentication key is generated. The **configuration file** is transmitted to CM only when the keys match mutually.

USE - For providing restricted transmission of **cable modem** (CM) **configuration file** maintained on trivial file transfer protocol (TFTP) server, for use with terminal such as personal computer and game console device.

ADVANTAGE - Unauthorized access to CM **configuration files** is reduced or eliminated.

DESCRIPTION OF DRAWINGS - The figure illustrates CM request and response for establishing IP connectivity.

Technology Focus

INDUSTRIAL STANDARDS - The authentication key is generated by encryption functions specified by data encryption standard (DES), data encryption algorithm (DEA), extended data encryption standard (DESX), advanced encryption standard (AES) including Rivest's Cipher (RC6), digital signature algorithm (DSA), RC2, RC4, RC5, secure hash algorithm (SHA), message digest algorithm (MD2,MD4,MD5), international data encryption algorithm (IDEA), secure and fast encryption routine (SAFER), fast data encipherment algorithm (FEAL), Skipjack, Blowfish, Carlisle Adams and Stafford Travares (CAST) and ElGamal. The encrypted wireless network conforms to ~IEEE 802.11~ .

Title Terms/Index Terms/Additional Words: CABLE; MODEM; TRANSMISSION; RESTRICT; METHOD; PERSON; COMPUTER; TRANSMIT; CONFIGURATION; FILE; AUTHENTICITY; KEY; GENERATE; BASED; MATCH

Class Codes
International Classification (Main): H04L-009/00
International Classification (+ Attributes)
IPC + Level Value Position Status Version
  H04L-0009/32 A I F   20060101
US Classification, Issued: 713200000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-C03A; T01-D01; T01-F05B2; W01-A05A

Cable modem **transmission restriction method for use with e.g. personal computer, involves transmitting** configuration file **to** cable modem **only if authentication keys generated based on** configuration file **match with each other**

Original Titles:
Method to block unauthorized access to TFTP server **configuration files**

Alerting Abstract ...NOVELTY - An unmodified **cable modem** (CM) **configuration filename** is associated to a CM internet protocol (IP) address and an authentication key is generated. A modified CM **configuration filename** is generated by combining previous filename with the key. The modified filename is parsed to unmodified filename by which a new authentication key is generated. The **configuration file** is transmitted to CM only when the keys match mutually.USE - For providing restricted transmission of **cable modem** (CM) **configuration file** maintained on trivial file transfer protocol (TFTP) server, for use with terminal such as personal...
...ADVANTAGE - Unauthorized access to CM **configuration files** is reduced or eliminated...

Original Publication Data by Authority

Original Abstracts:
The present invention teaches methods and systems for blocking unauthorized access to **cable modem configuration files stored on trivial file** transfer protocol (TFTP) servers. Filenames are modified by the DHCP to incorporate an authentication key (and optional cloaking) prior to transmission to the **cable modem** . When the **TFTP server** receives a modified filename, it also generates an authentication key. The authentication keys must match in order for the **cable modem** to receive **the configuration file** requested. At **a minimum** , authentication keys depend upon the un-modified filename, the **cable modem IP address and a " coordination pass** phrase" known to the TFTP server and DHCP server, but not known to the **cable modem** . Variations include **optional cloaking** , various actions performed for non-matching authentication keys, selection of authentication key generating algorithm and inclusion of **cable** modem MAC address in the authentication key for all **cable modems** or for **premium service** customer **cable modems.** >
Claims:
What is claimed is:<b>1</b>. A method for providing restricted transmissions of **cable modem** (CM) **configuration files** maintained on a trivial **file transfer** protocol **server** (**TFTP**), the method comprising:using **a** dynamic host **configuration** protocol (DHCP) server to associate an un-modified CM **configuration filename** to a **cable modem** Internet protocol (**IP**) **address** upon **receipt of** a DHCP **REQUEST ;**

storing a coordination **pass phrase** on a DHCP server and a TFTP server;generating a **first authentication key** ;creating a modified CM **configuration filename** by combining a CM **configuration filename with the authentication key** ;transmitting the modified CM **configuration filename to** the **cable modem** in **a DHCP** RESPONSE;transmitting the modified CM **configuration** filename from the **cable modem to** the TFTP **server** ; **parsing** the modified CM **configuration filename** into the un-modified CM **configuration** filename ;generating a **second authentication key** ;transmitting the CM **configuration file** to the **cable modem only if** the **first authentication key matches** the second **authentication key** ;wherein the **first authentication key** and the second **authentication key depend upon** the un- **modified** CM configuration filename, the **cable modem IP address** and the **coordination pass** phrase.

10/69,K/4 **(Item 4 from file: 350)**
DIALOG(R)File 350:Derwent WPIX

0014763117 - Drawing available
WPI ACC NO: 2005-110771/200512
XRPX Acc No: N2005-095681

Cable modem **transmission restriction method for use with e.g. personal computer, involves transmitting** configuration file **to** cable modem **only if authentication keys generated based on** configuration file **match with each other**

Patent Assignee: DANFORTH A (DANF-I); GOULD K (GOUL-I); TIME WARNER CABLE INC (TIME-N)
Inventor: DANFORTH A; GOULD K

Patent Family (2 patents, 2 countries)

Patent			Application				
Number	Kind	Date	Number	Kind	Date	Update	
US 20050005154	A1	20050106	US 2003613659	A	20030703	200512	B
CA 2473326	A1	20060108	CA 2473326	A	20040708	200612	NCE

Priority Applications (no., kind, date): CA 2473326 A 20040708; US 2003613659 A 20030703

Patent Details

Number	Kind	Lan	Pg	Dwg	Filing Notes
US 20050005154	A1	EN	22	9	
CA 2473326	A1	EN			

Alerting Abstract US A1

NOVELTY - An unmodified **cable modem** (CM) **configuration filename** is associated to a CM internet protocol (IP) address and an authentication key is generated. A modified CM **configuration filename** is generated by combining previous filename with the key. The modified filename is parsed to unmodified filename by which a new authentication key is generated. The **configuration file** is transmitted to CM only when the keys match mutually.

USE - For providing restricted transmission of **cable modem** (CM) **configuration file** maintained on trivial file transfer protocol (TFTP) server, for use with terminal such as personal computer and game console device.

ADVANTAGE - Unauthorized access to CM **configuration files** is reduced or eliminated.

DESCRIPTION OF DRAWINGS - The figure illustrates CM request and response for establishing IP connectivity.

Technology Focus

INDUSTRIAL STANDARDS - The authentication key is generated by encryption functions specified by data encryption standard (DES), data encryption algorithm (DEA), extended data encryption standard (DESX), advanced encryption standard (AES) including Rivest's Cipher (RC6), digital signature algorithm (DSA), RC2, RC4, RC5, secure hash algorithm (SHA), message digest algorithm (MD2,MD4,MD5), international data encryption algorithm (IDEA), secure and fast encryption routine (SAFER), fast data encipherment algorithm.(FEAL), Skipjack, Blowfish, Carlisle Adams and Stafford Travares (CAST) and ElGamal. The encrypted wireless network conforms to ~IEEE 802.11~ .

Title Terms/Index Terms/Additional Words: CABLE; MODEM; TRANSMISSION; RESTRICT; METHOD; PERSON; COMPUTER; TRANSMIT; CONFIGURATION; FILE; AUTHENTICITY; KEY; GENERATE; BASED; MATCH

Class Codes
International Classification (Main): H04L-009/00
International Classification (+ Attributes)
IPC + Level Value Position Status Version
H04L-0009/32 A I F 20060101
US Classification, Issued: 713200000

File Segment: EPI;
DWPI Class: T01; W01
Manual Codes (EPI/S-X): T01-C03A; T01-D01; T01-F05B2; W01-A05A

Cable modem **transmission restriction method for use with e.g. personal computer, involves transmitting** configuration file **to** cable modem **only if authentication keys generated based on** configuration file **match with each other**

Original Titles:
Method to block unauthorized access to TFTP server **configuration files**

Alerting Abstract ...NOVELTY - An unmodified **cable modem** (CM) **configuration filename** is associated to a CM internet protocol (IP) address and an authentication key is generated. A modified CM **configuration filename** is generated by combining previous filename with the key. The modified filename is parsed to unmodified filename by which a new authentication key is generated. The **configuration file** is transmitted to CM only when the keys match mutually.USE - For providing restricted transmission of **cable modem** (CM) **configuration file** maintained on trivial file transfer protocol (TFTP) server, for use with terminal such as personal...
...ADVANTAGE - Unauthorized access to CM **configuration files** is reduced or eliminated...

Original Publication Data by Authority

Original Abstracts:
The present invention teaches methods and systems for blocking unauthorized access to **cable modem configuration files stored on trivial file** transfer protocol (TFTP) servers. Filenames are modified by the DHCP to incorporate an authentication key (and optional cloaking) prior to transmission to the **cable modem** . When the **TFTP server** receives a modified filename, it also generates an authentication key. The authentication keys must match in order for the **cable modem** to receive **the configuration file** requested. At **a minimum** , authentication keys depend upon the un-modified filename, the **cable modem IP address and a " coordination pass** phrase" known to the TFTP server and DHCP server, but not known to the **cable modem** . Variations include **optional cloaking** , various actions performed for non-matching authentication keys, selection of authentication key generating algorithm and inclusion of **cable** modem MAC address in the authentication key for all **cable modems** or for **premium service** customer **cable modems**. >
Claims:
What is claimed is:<b>1</b>. A method for providing restricted transmissions of **cable modem** (CM) **configuration files** maintained on a trivial **file transfer** protocol **server** (**TFTP**), the method comprising:using **a** dynamic host **configuration** protocol (DHCP) server to associate an un-modified CM **configuration filename** to a **cable modem** Internet protocol (**IP**) **address** upon **receipt of** a DHCP **REQUEST ;**

storing a coordination **pass phrase** on a DHCP server and a TFTP server;generating a **first authentication key** ;creating a modified CM **configuration filename** by combining a CM **configuration filename with the authentication key** ;transmitting the modified CM **configuration filename to** the **cable modem** in **a DHCP** RESPONSE;transmitting the modified CM **configuration** filename from the **cable modem to** the TFTP **server** ; **parsing** the modified CM **configuration filename** into the un-modified CM **configur**ation filename ;generating a **second authentication key** ;transmitting the CM **configuration file** to the **cable modem only if** the **first authentication key matches** the second **authentication key** ;wherein the **first authentication key** and the second **authentication key depend upon** the un- **modified** CM configuration filename, the **cable modem IP address** and the **coordination pass** phrase.

```
Set     Items   Description
S1     806213    ((CABLE OR DATA)()MODEM? OR CABLE? OR COMMUNICATION? OR DA-
             TA OR HIGH???()SPEED? OR BROADBAND OR HOOK()UP)(3N)(MODEM? OR
             DEVICE? OR INSTRUMENT? OR MECHANISM? OR MACHINE? ? OR UNIT? OR
              APPARAT? OR HARDWARE?)
S2      55564    (KEY? ? OR DEVICE OR MECHANISM?? OR PASSWORD?? OR CODE? ? -
             OR CODING OR ACCESS?)(5N)(CERTIF? OR AUTHENTIC? OR VERIF? OR -
             VALID? OR AUTHORI?)
S3       8095   S2(3N)(ONE OR FIRST? OR 1ST OR PRIMARY OR INITIAL? OR ORIG-
             INAL? OR MAIN OR REFER? OR SOURC?)
S4       2438   S3(5N)(MATCH? OR EQUATE? OR EQUATING OR PAIR OR COORDINAT?
             OR CORRESPOND? OR IDENT? OR SQUARE? OR MATE? ? OR CORRELAT? OR
              SAME OR MUTUAL? OR DEPEND? OR BASE? ? OR DERIV?)
S5       6677   S2(3N)(SECOND? OR COUPLE OR 2ND OR 2 OR TWICE OR ANOTHER? -
             OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADDITIONAL)
S6     165885    ((SET OR SETT??? OR SETS)()(UP OR UPS) OR PARAMETER? ? OR -
             SETTING? ? OR CONFIGUR? OR PROPERT? OR OPTION? OR PROFIL? OR -
             PREFEREN?)(3N)(FILE? OR DATA OR INFORMATION OR INFO)
S7      28771   S6(5N)(DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT?
              OR TRANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?)
S8      36717   S6(5N)(RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR PULL???-
             ()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV? OR AC-
             CESS?)
S9      10602   S1(2N)(IPADDRESS? OR (INTERNET()PROTOCOL OR IP OR LOGICAL -
             OR DOT OR NETWORK?)()ADDRESS? OR ADDRESS?)
S10         9   S3:S4 AND S5 AND S1 AND S6 AND S9
File 350:Derwent WPIX 1963-2007/UD=200752
         (c) 2007 The Thomson Corporation
File 347:JAPIO Dec 1976-2007/Mar(Updated 070809)
         (c) 2007 JPO & JAPIO
```

```
Set     Items   Description
S1     306100   ((CABLE OR DATA)()MODEM? OR CABLE? OR COMMUNICATION? OR DA-
             TA OR HIGH???()SPEED? OR BROADBAND OR HOOK()UP)(3N)(MODEM? OR
             DEVICE? OR INSTRUMENT? OR MECHANISM? OR MACHINE? ? OR UNIT? OR
              APPARAT? OR HARDWARE?)
S2      73739   (KEY? ? OR DEVICE OR MECHANISM?? OR PASSWORD?? OR CODE? ? -
             OR CODING OR ACCESS?)(5N)(CERTIF? OR AUTHENTIC? OR VERIF? OR -
             VALID? OR AUTHORI?)
S3       3468   S2(3N)(ONE OR FIRST? OR 1ST OR PRIMARY OR INITIAL? OR ORIG-
             INAL? OR MAIN OR REFER? OR SOURC?)
S4        504   S3(5N)(MATCH? OR EQUATE? OR EQUATING OR PAIR OR COORDINAT?
              OR CORRESPOND? OR IDENT? OR SQUARE? OR MATE? ? OR CORRELAT? OR
              SAME OR MUTUAL? OR DEPEND? OR BASE? ? OR DERIV?)
S5       3913   S2(3N)(SECOND? OR COUPLE OR 2ND OR 2 OR TWICE OR ANOTHER? -
             OR TWO OR DIFFERENT OR PAIR OR MORE(2N)ONE OR ADDITIONAL)
S6     261284   ((SET OR SETT??? OR SETS)()(UP OR UPS) OR PARAMETER? ? OR -
             SETTING? ? OR CONFIGUR? OR PROPERT? OR OPTION? OR PROFIL? OR -
             PREFEREN?)(3N)(FILE? OR DATA OR INFORMATION OR INFO)
S7      14698   S6(5N)(DELIVER? OR SEND??? OR SENT OR UPLOAD? OR DISTRIBUT?
              OR TRANSFER? OR TRANSMI? OR BEAM??? OR LOAD??? OR POST??? ?)
S8      19978   S6(5N)(RECEIV? OR ACCEPT? OR ACQUIR? OR OBTAIN? OR PULL???-
             ()DOWN?? OR PROCUR??? OR GET? ? OR FETCH??? OR RETRIEV? OR AC-
             CESS?)
S9        581   S1(2N)(IPADDRESS? OR (INTERNET()PROTOCOL OR IP OR LOGICAL -
             OR DOT OR NETWORK?)()ADDRESS? OR ADDRESS?)
S10         0   S3:S4 AND S5 AND S1 AND S6 AND S9
File   2:INSPEC 1898-2007/Aug W1
         (c) 2007 Institution of Electrical Engineers
File   6:NTIS 1964-2007/Aug W3
         (c) 2007 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1884-2007/Aug W1
         (c) 2007 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2007/Aug W3
         (c) 2007 The Thomson Corp
File  35:Dissertation Abs Online 1861-2007/Jul
         (c) 2007 ProQuest Info&Learning
File  56:Computer and Information Systems Abstracts 1966-2007/Aug
         (c) 2007 CSA.
File  60:ANTE: Abstracts in New Tech & Engineer 1966-2007/Jul
         (c) 2007 CSA.
File  62:SPIN(R) 1975-2007/Jul W5
         (c) 2007 American Institute of Physics
File  65:Inside Conferences 1993-2007/Aug 15
         (c) 2007 BLDSC all rts. reserv.
File  95:TEME-Technology & Management 1989-2007/Aug W2
         (c) 2007 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2007/Jul
         (c) 2007 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2007/Aug 08
         (c) 2007 The Gale Group
File 144:Pascal 1973-2007/Jul W5
         (c) 2007 INIST/CNRS
File 239:Mathsci 1940-2007/Sep
         (c) 2007 American Mathematical Society
File 256:TecInfoSource 82-2007/Nov
         (c) 2007 Info.Sources Inc
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 2006 The Thomson Corp
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
```